WHAT IS CLAIMED IS:

1. A method for multiplying two elements of a finite field, the method comprising the steps of:

mapping two input operands into a composite finite field that is defined by a first irreducible polynomial of degree m*n, the first irreducible polynomial being defined by using a ground field that is defined by a second irreducible polynomial of degree n and by using an extension field that is defined by a third irreducible polynomial of degree m;

performing an initial KOA processing upon the two input operands in order to prepare the two input operands for multiplication in the ground field; and

performing multiplication in the ground field using a triangular basis multiplier.

2. The method of claim 1, wherein the step of performing the initial KOA processing includes the sub-step of:

transforming an input vector including four sub-elements (a_0, a_1, a_2, a_3) into an intermediate vector that is defined by:

$$\begin{pmatrix} a_0 \\ a_0 + a_1 \\ a_1 \\ a_0 + a_2 \\ \text{----} \\ a_0 + a_1 + a_2 + a_3 \\ a_1 + a_3 \\ a_2 \\ a_2 + a_3 \\ \text{--------} \\ a_3 \\ x \\ x \\ x \end{pmatrix}$$

wherein the "+" operator represents a bit-wise exclusive-OR operation and "x" indicates unused or undefined values.

3. The method of claim 1, further comprising the step of performing a final KOA processing that is divided into a plurality of uniform subsets such that the uniform subsets are scalable for processing of different values of m used to define the extension field.

4. The method of claim 1, further comprising the step of defining the first, second, and third irreducible polynomials.

5. A method for multiplying two elements of a finite field, the method comprising the steps of:

mapping two input operands into a composite finite field that is defined by a first irreducible polynomial of degree m*n, the first irreducible polynomial being defined by using a ground field that is defined by a second irreducible polynomial of degree n and by using an extension field that is defined by a third irreducible polynomial of degree m;

performing an initial KOA processing upon each of the two input operands in order to prepare the two input operands for multiplication in the ground field, the initial KOA processing being divided into a plurality of uniform subsets such that the uniform subsets are scalable for processing of different values of m used to define the extension field; and

performing a subsequent multiplication processing upon a result of the initial KOA processing to produce a multiplicative product over the composite finite field.

6. The method of claim 5, wherein the step of performing the initial KOA processing includes the sub-step of producing a plurality of output operands that each are within the ground field.

7. The method of claim 5, further comprising the step of defining the first, second, and third irreducible polynomials.

8. A Galois field multiplier comprising:

an input operand mapper for mapping two input operands into a composite finite field that is defined by a first irreducible polynomial of degree m*n, the first irreducible polynomial being defined by using a ground field that is defined by a second irreducible polynomial of degree n and by using an extension field that is defined by a third irreducible polynomial of degree m;

an initial KOA processor for performing an initial KOA processing upon the two input operands in order to prepare the two input operands for multiplication in the ground field; and

a triangular basis ground field multiplier for performing multiplication in the ground field.

9. The Galois field multiplier of claim 8,

wherein the initial KOA processor transforms an input vector including four sub-elements (a_0, a_1, a_2, a_3) into an intermediate vector defined by:

$$\begin{pmatrix} a_0 \\ a_0 + a_1 \\ a_1 \\ a_0 + a_2 \\ \text{----} \\ a_0 + a_1 + a_2 + a_3 \\ a_1 + a_3 \\ a_2 \\ a_2 + a_3 \\ \text{--------} \\ a_3 \\ x \\ x \\ x \end{pmatrix}$$

wherein the "+" operator represents a bit-wise exclusive-OR operation and "x" indicates unused or undefined values.

10. The Galois field multiplier of claim 8, further comprising a final KOA processor for performing a final KOA processing that is divided into a plurality of uniform subsets such that the uniform subsets are scalable for processing of different values of m used to define the extension field.

11. The Galois field multiplier of claim 8, wherein the first, second, and third irreducible polynomials are used-defined.

12. A finite field data multiplier for multiplying two elements of a finite field, the multiplier comprising:

an input operand mapper for mapping two input operands into a composite finite field that is defined by a first irreducible polynomial of degree m*n, the first irreducible polynomial being defined by using a ground field that is defined by a second irreducible polynomial of degree n and by using an extension field that is defined by a third irreducible polynomial of degree m;

an initial KOA processor for performing an initial KOA processing upon each of the two input operands in order to prepare the two input operands for multiplication in the ground field, the initial KOA processor dividing the input operands into a plurality of uniform subsets such that the uniform subsets are scalable for processing of different values of m used to define the extension field; and

a multiplier means for performing a subsequent multiplication processing upon a result from the initial KOA processor to produce a multiplicative product over the composite finite field.

13. The multiplier of claim 12, wherein the initial KOA processor produces a plurality of output operands that each are within the ground field.

14. The multiplier of claim 12, wherein the first, second, and third irreducible polynomials are used-defined.

15. A machine-readable medium encoded with a program for multiplying two elements of a finite field, said program containing instructions for performing the steps of:

mapping two input operands into a composite finite field that is defined by a first irreducible polynomial of degree m*n, the first irreducible polynomial being defined by using a ground field that is defined by a second irreducible polynomial of degree n and by using an extension field that is defined by a third irreducible polynomial of degree m;

performing an initial KOA processing upon the two input operands in order to prepare the two input operands for multiplication in the ground field; and

performing multiplication in the ground field using a triangular basis multiplier.

16. The machine-readable medium of claim 15, wherein the step of performing the initial KOA processing includes the sub-step of:

transforming an input vector including four sub-elements (a_0, a_1, a_2, a_3) into an intermediate vector that is defined by:

$$\begin{pmatrix} a_0 \\ a_0 + a_1 \\ a_1 \\ a_0 + a_2 \\ \text{----} \\ a_0 + a_1 + a_2 + a_3 \\ a_1 + a_3 \\ a_2 \\ a_2 + a_3 \\ \text{--------} \\ a_3 \\ x \\ x \\ x \end{pmatrix}$$

wherein the "+" operator represents a bit-wise exclusive-OR operation and "x" indicates unused or undefined values.

17. The machine-readable medium of claim 15, wherein said program further contains instructions for performing the step of performing a final KOA processing that is divided into a plurality of uniform subsets such that the uniform subsets are scalable for processing of different values of m used to define the extension field.

18. A machine-readable medium encoded with a program for multiplying two elements of a finite field, said program containing instructions for performing the steps of:

mapping two input operands into a composite finite field that is defined by a first irreducible polynomial of degree m*n, the first irreducible polynomial being defined by using a ground field that is defined by a second irreducible polynomial of degree n and by using an extension field that is defined by a third irreducible polynomial of degree m;

performing an initial KOA processing upon each of the two input operands in order to prepare the two input operands for multiplication in the ground field, the initial KOA processing being divided into a plurality of uniform subsets such that the uniform subsets are scalable for processing of different values of m used to define the extension field; and

performing a subsequent multiplication processing upon a result of the initial KOA processing to produce a multiplicative product over the composite finite field.

19. The machine-readable medium of claim 18, wherein the step of performing the initial KOA processing includes the sub-step of producing a plurality of output operands that each are within the ground field.

20. A method for multiplying two elements of a finite field that is redefinable, the method comprising the steps of:

switching data bit ordering of a plurality of data bits representing a first multiplicand, such that a most significant bit of the first multiplicand is placed into a rightmost position regardless of the number of bits in the plurality of data bits representing the first multiplicand, successively less significant bits are placed into successive bits to the left of the most significant bit, and unused bits are set to zero;

converting the first multiplicand from an initial basis into a triangular basis;

switching data bit ordering of a plurality of coefficient bits representing each of a plurality of coefficients in a Galois Field generator polynomial that defines a Galois Field over which multiplication is to be performed, such that a most significant bit of each of the coefficients is placed into a rightmost position regardless of the number of bits in the plurality of coefficient bits, successively less significant bits are placed into successive bits to the left of the most significant bit, and unused bits are set to zero;

performing multiplication based upon at least the first multiplicand and a second multiplicand to produce a multiplication result; and

converting the multiplication result from triangular basis to the initial basis.

21. The method of claim 20, wherein the step of performing multiplication includes the sub-steps of:

generating a Hankel Matrix based upon the first multiplicand and the plurality of coefficients; and

multiplying the Hankel matrix with a second multiplicand to produce the multiplication result.

22. The method of claim 20, wherein the step of switching data bit ordering of a plurality of data bits includes the step of selecting a plurality of outputs from a plurality of data multiplexers, the plurality of data multiplexers including one data multiplexer for each data bit in the plurality of data bits.

23. A machine-readable medium encoded with a program for performing the method of claim 20.

24. A flexible Galois field multiplier for multiplying two elements of a finite field that is redefinable, the multiplier comprising:

a first switching circuit for switching data bit ordering of a plurality of data bits representing a first multiplicand, the first switching circuit placing a most significant bit of the first multiplicand into a rightmost position regardless of the number of bits in the plurality of data bits representing the first multiplicand, placing successively less significant bits into successive bits to the left of the most significant bit, and setting unused bits to zero;

a first basis converter for converting the first multiplicand from an initial basis into a triangular basis;

a second switching circuit for switching data bit ordering of a plurality of coefficient bits representing each of a plurality of coefficients in a Galois Field generator polynomial that defines a Galois Field over which multiplication is to be performed, the second switching circuit placing a most significant bit of each of the coefficients into a rightmost position regardless of the number of bits in the plurality of coefficient bits, placing successively less significant bits into successive bits to the left of the most significant bit, and setting unused bits to zero;

a multiplier for performing multiplication based upon at least the first multiplicand and a second multiplicand to produce a multiplication result; and

a second basis converter for converting the multiplication result from triangular basis to the initial basis.

25. The multiplier of claim 24, wherein the multiplier generates a Hankel Matrix based upon the first multiplicand and the plurality of coefficients, and multiplies the Hankel matrix with a second multiplicand to produce the multiplication result.

26. The multiplier of claim 24, wherein the first switching circuit includes a plurality of data multiplexers, the plurality of data multiplexers including one data multiplexer for each data bit in the plurality of data bits.

27. A modulo reduction processor for performing modulo reduction within a finite field of an unreduced data element, the finite field having a dimension equal to an integer multiple of n, the modulo reduction processor comprising:

a reduction matrix generator;

a matrix restructurer for restructuring the reduction matrix into a column vector, such that each element of the column vector is a quantity including one or more values that each are up to n bits in length; and

a reducer for reducing the data element by performing a combination of the data element and the column vector.

28. The modulo reduction processor of claim 27,

wherein the reducer includes a multiply-accumulate processing module for performing the combination of the data element and the column vector, the multiply-accumulate processing module being optimized for processing inputs of order n, and

the data element is an integer multiple of n that is greater than two.

29. The modulo reduction processor of claim 27,

wherein the reducer includes an n-bit exclusive-OR processing module for performing the combination of the data element and the column vector, and

the data element is an integer multiple of n that is greater than two.

30. A machine-readable medium encoded with a program for performing modulo reduction within a finite field of an unreduced data element, the finite field having a dimension equal to an integer multiple of n, said program containing instructions for performing the steps of:

generating a reduction matrix;

restructuring the reduction matrix into a column vector, each element of the column vector being a quantity including one or more values that each are up to n bits in length; and

reducing the data element by performing a combination of the data element and the column vector.

31. The machine-readable medium of claim 30,

wherein in the step of reducing the data element, the combination of the data element and the column vector is performed using one or more multiply-accumulate processing modules that are optimized for processing inputs of order n, and

the data element is an integer multiple of n that is greater than two.

32. The machine-readable medium of claim 30,

wherein in the step of reducing the data element, the combination of the data element and the column vector is performed using one or more n-bit exclusive-OR processing modules, and

the data element is an integer multiple of n that is greater than two.